Método de autenticación seguro de usuarios de base de datos y de sistema para el desarrollo de aplicaciones web en empresas

@jofrantoba

Visión General

- Realidad Problemática.
- Identificando Problema.
- Objetivos.
- Hipótesis.
- Solución.
- Beneficios.
- Conclusiones.
- Recomendaciones

Realidad problemática



Los desarrolladores no salvaguardan los datos de conectividad a los servicios de almacenamiento

Identificando problema

¿Cómo mantener la confidencialidad de los datos de conectividad al servicio de almacenamiento para el desarrollo de software?

Objetivos

- Objetivo General:
  - Desarrollar un método de autenticación seguro de usuarios, el cual permita asegurar la confidencialidad de los datos de conectividad al servicio de almacenamiento.
- Objetivos Específicos:
  - Crear y diseñar un método seguro de autenticación, que permita asegurar la confidencialidad de los datos de conectividad.
  - Desarrollar un sistema que implemente un método seguro de autenticación de usuarios de base de datos y de sistema.

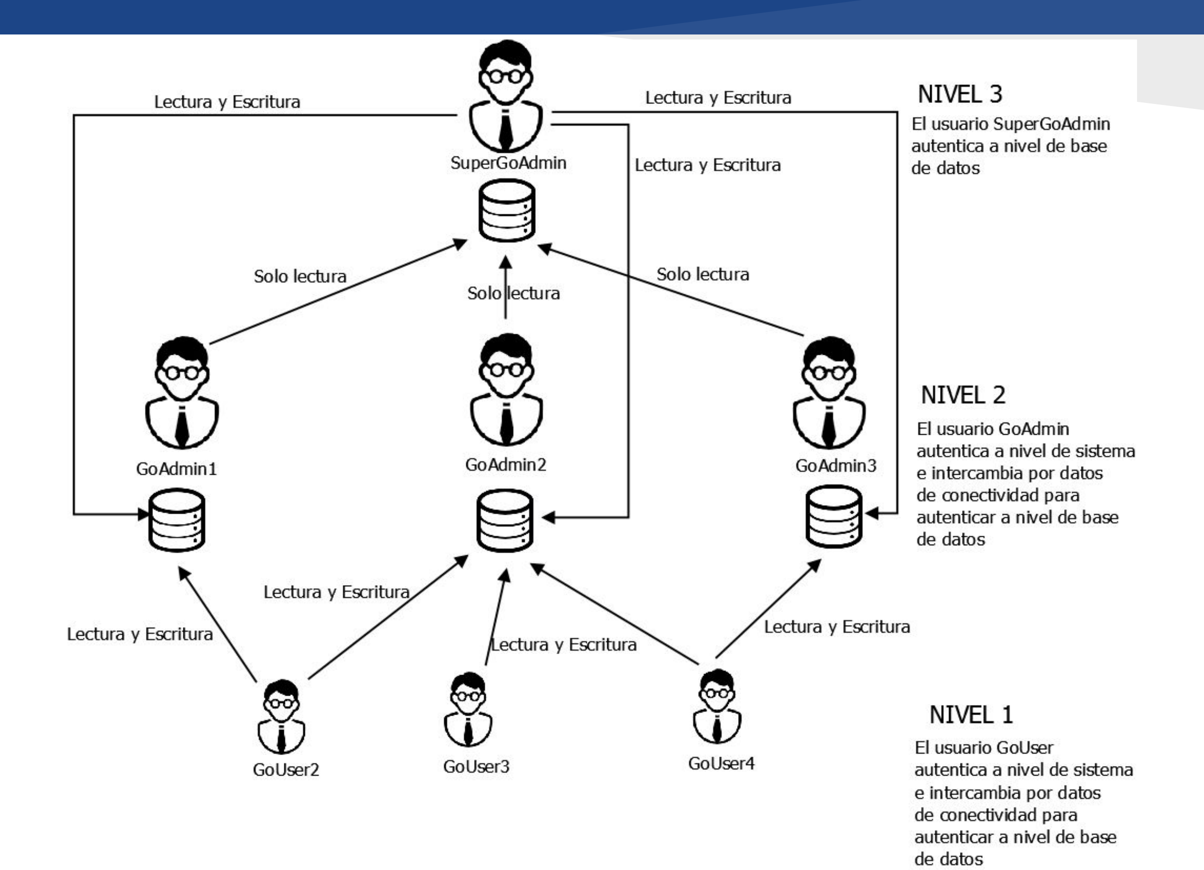
Hipótesis

Implementar un método de autenticación que permita salvaguardar los datos de conectividad al servicio de almacenamiento en la memoria RAM del servidor, disminuyendo así el riesgo de robo de datos de conectividad y por ende acceso no autorizado al almacén de datos.

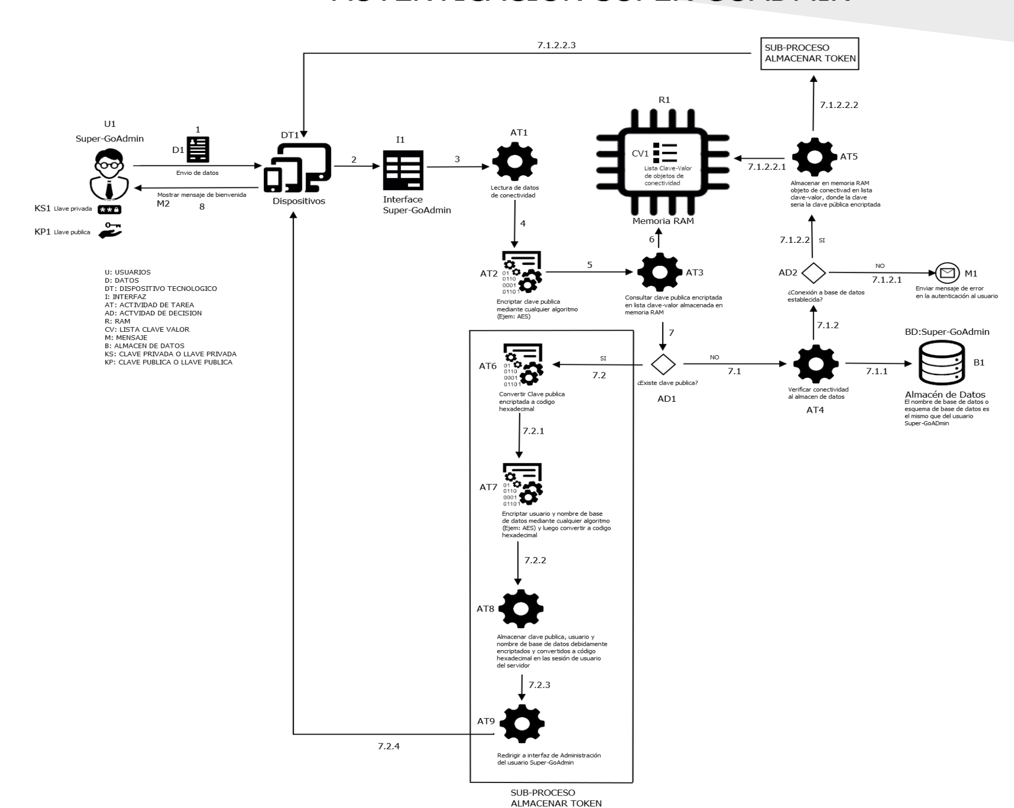
Solución

Método de autenticación por clave pública ó método de autenticación GO

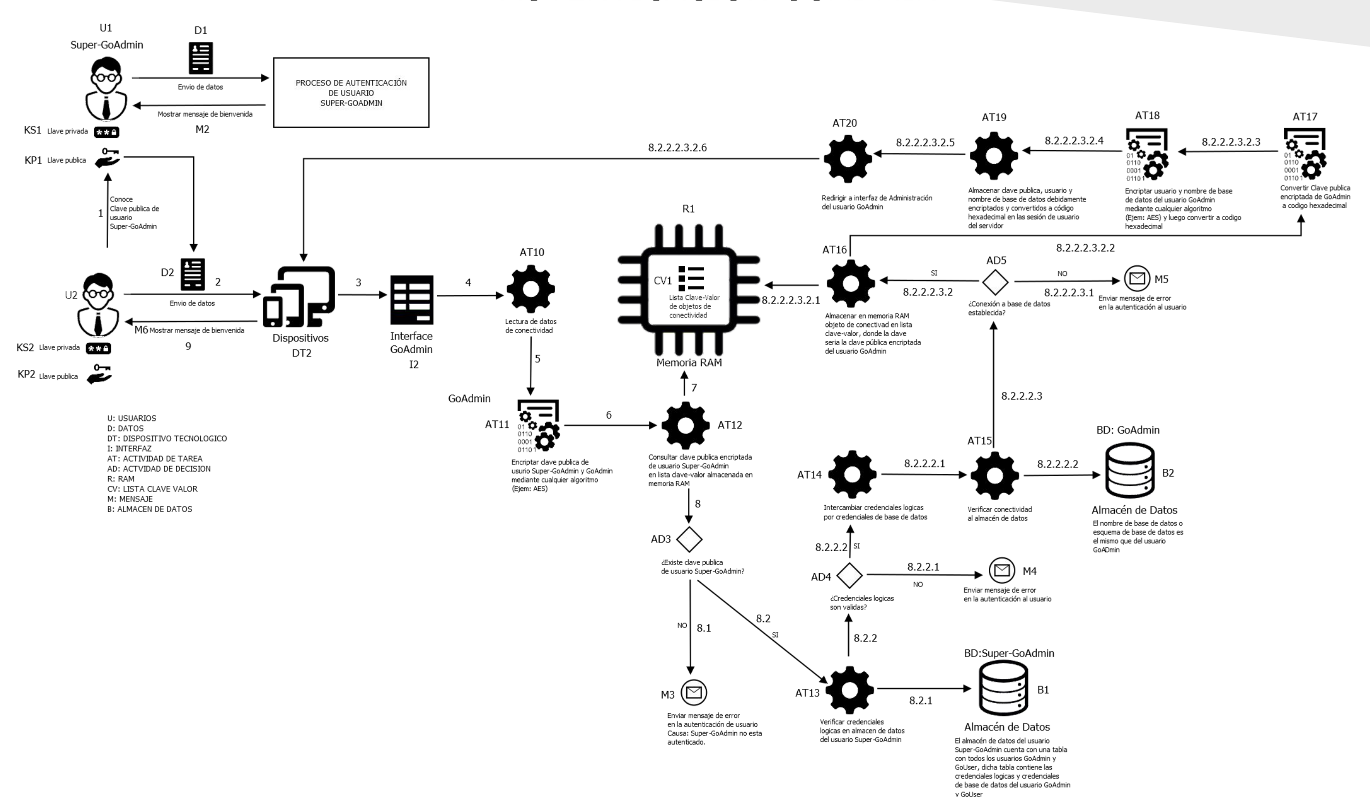
Solución: Autenticación basada en 3 niveles



Solución: Autenticando SuperGoAdmin

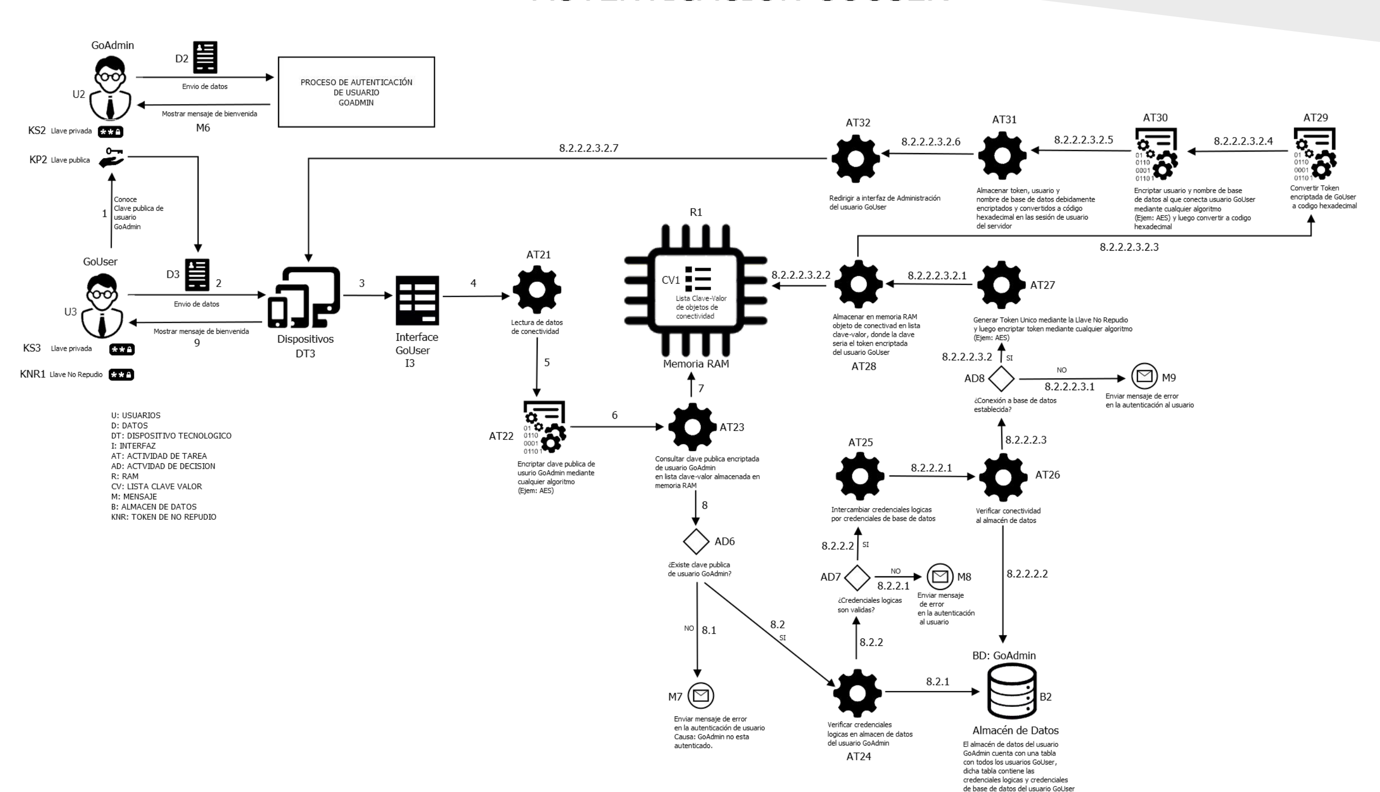


Solución: Autenticando GoAdmin



Solución: Autenticando GoUser

AUTENTICACIÓN GOUSER



Solución

Desarrollo de sistema que implemente el método de autenticación por clave pública.

Beneficios

Mantener seguros los datos de conectividad al servicio de almacenamiento.



Beneficios

Alta performance en conectividad a base de datos.

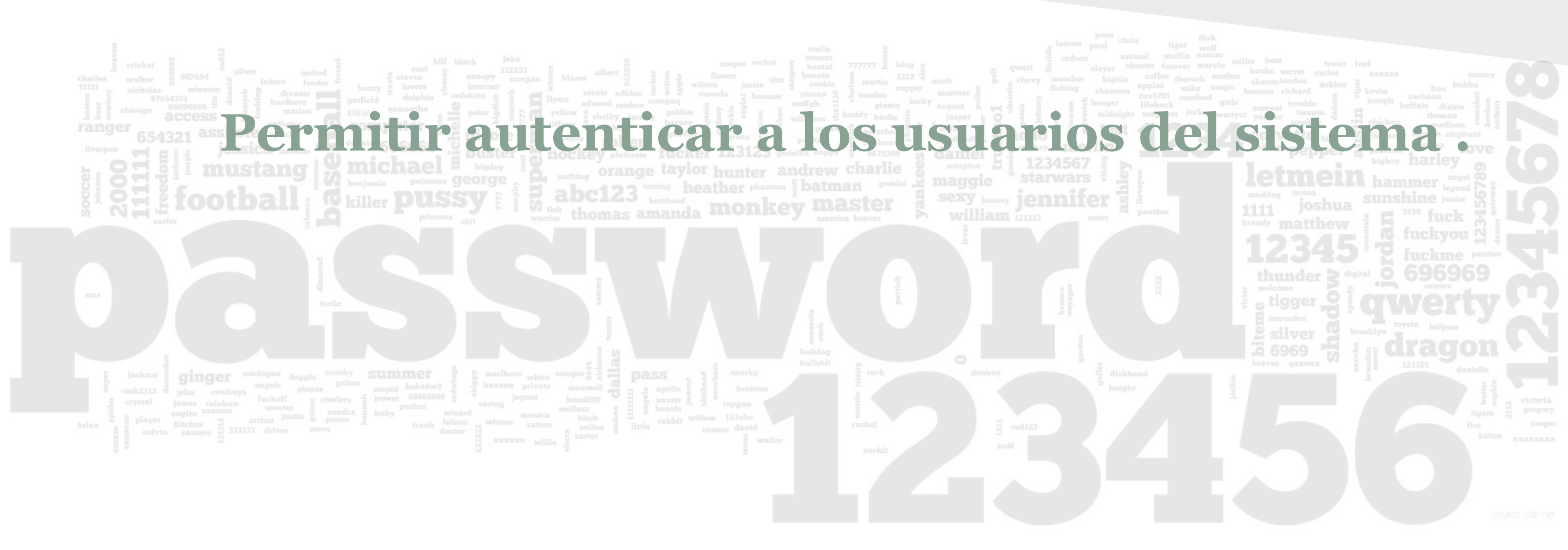


Beneficios



Seguridad de autenticación basada en 3 niveles.

Beneficios



Permitir autenticar a los usuarios del sistema .

Beneficios

Administración centralizada de usuarios.

Beneficios

Control y monitoreo de usuarios a nivel de sistema y de actividad SQL.

Beneficios

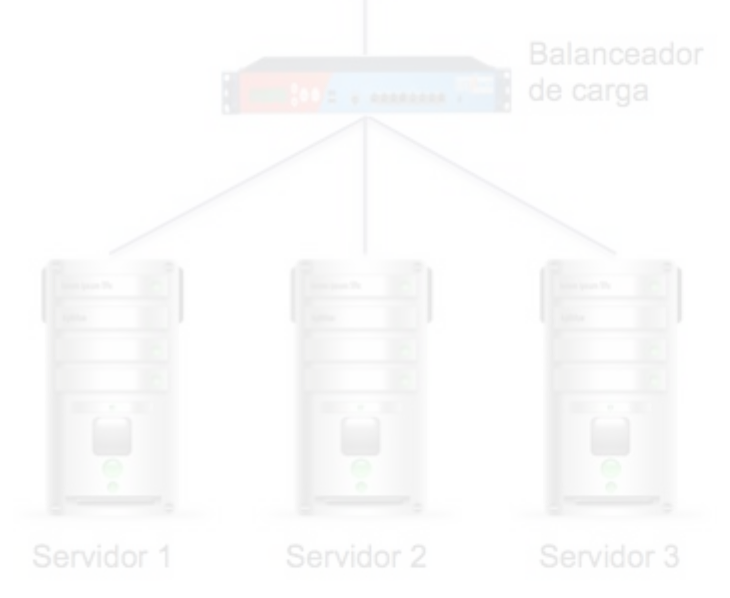
Control de número de conexiones y sesiones abiertas en el almacén de datos y Servidor de aplicaciones.

Beneficios

Dinamismo físico y lógico del servicio de almacenamiento.

Beneficios

Permite desarrollar balanceo de carga.



Beneficios

Permite desarrollar un DAM (Database activity monitor).

Beneficios

No repudio al autenticar.

Conclusiones

Guardar los datos de conectividad en la memoria RAM de los servidores, permite disminuir las probabilidades de robo de estos datos.

Conclusiones

Al implementar un método de autenticación basada en 3 niveles de seguridad, proporciona características que permiten monitorear y controlar los accesos al sistema.

Conclusiones

El método permite balancear la carga tanto en conexiones a base de datos como a nivel de servidores de aplicaciones, ya que los datos de conectividad son enviados y no almacenados en el código fuente o archivos de texto plano.

Conclusiones

Monitorear la actividad SQL es una las características que proporciona este método de autenticación.



Conclusiones

Controlar el número de conexión o sesiones abierta con los servicios de almacenamiento garantiza el rendimiento de las aplicaciones implementadas con este método.

Recomendaciones

No exponer los datos de conectividad al servicio de almacenamiento en el código fuente, ni en archivos de texto plano.

Recomendaciones

No usar tecnología de conectividad de almacenamiento de datos que obliguen a exponer los datos de conectividad en los clientes.

Recomendaciones

Como desarrolladores, se debe salvaguardar esta información y jamás difundirla.


@jofrantoba